




 Quick Actions


 [Support Home](#)


 [Support Cases](#)


 Account Management


 Members

 Assets

 Tools

 WildFire

 Updates

 Resources

Enable System and Network Extensions using jamf PRO

Created On 08/26/20 21:16 PM - Last Modified 01/20/21 07:25 AM  4773

[GLOBALPROTECT AGENT](#) [INSTALLATION](#) [GLOBALPROTECT](#) [PRISMA ACCESS](#)

Symptom Background

GlobalProtect App starting 5.1.4 uses system extensions on macOS Catalina 10.15.4 or later endpoints for enabling capabilities such as:

- [Split tunnel](#) based on the destination domain name and application process name
- Enforce GlobalProtect connections for network access (see [GlobalProtect App Customization](#)) without requiring [kernel extensions](#)

GlobalProtect App starting 5.2 uses system extensions on macOS Catalina 10.15.4 or later endpoints for enabling capabilities such as:

- [Split DNS](#)

When GlobalProtect app is installed on a macOS Catalina 10.15.4 or later device for the first time or is upgraded to GlobalProtect app 5.1.4, they must now enable the [system extensions](#). If you have configured split tunnel on the gateway or enforced GlobalProtect connections for network access on the portal, the **System Extension Blocked** notification message displays on the app during the installation, prompting users to enable and allow the system extensions in macOS that are blocked from loading to use these GlobalProtect features.

Objective:

Objective of this document is to utilize GlobalProtect 5.1.6 signed configuration profiles and deploy them using jamf PRO to suppress macOS 10.15.4 or later system and network extension pop-ups. The workflow can be used for any other Mobile Device Manager (MDM) provider which supports deploying configuration profiles.

Note: *This document assumes that the macOS endpoint does not have network extensions enabled manually. If network extensions are already enabled manually via GlobalProtect pop-up's than using configuration profile, via jamf PRO, to enable network extensions will create a duplicate network extension entries.*

Environment

- GlobalProtect 5.1.6 or later
- macOS Catalina 10.15.4 or later / macOS BigSur 11.

Prerequisite:

- jamf PRO Configuration profiles are supported with GlobalProtect 5.1.6 and onwards only.
- macOS Catalina 10.15.4 or later / macOS BigSur 11.
- Before using the configuration profile files, please make sure that the file is not corrupted by verifying the hash of the downloaded file with the hash provided for each file in this document and making sure they both match. If otherwise please re-download the files.

Resolution

Table of Contents:

- [Enable GlobalProtect System Extension](#)
- [Enable GlobalProtect Network Extension on macOS Catalina 10.15.4 and later Endpoints](#)
- [Enable GlobalProtect Network Extension on macOS BigSur 11 Endpoints](#)
- [Steps for Adding a Configuration Profile for Enforcer on jamfPro v10.26.0](#)
- [Verify Configuration Profiles](#)

Enable GlobalProtect System Extension:

- Upon successful installation of GlobalProtect Client, following system extension pop-up will be seen as explained in [GlobalProtect app guide](#).

Other users also viewed:

[Allow System Extension for MacOSX Catalina 10.15.4 or later](#)

[Enhanced Security on macOS Catalina 10.15](#)

[Error message: “System Extension Blocked” seen on macOS endpoints during GlobalProtect installation](#)

[GlobalProtect Portal Fails to Generate Cookie](#)



Actions

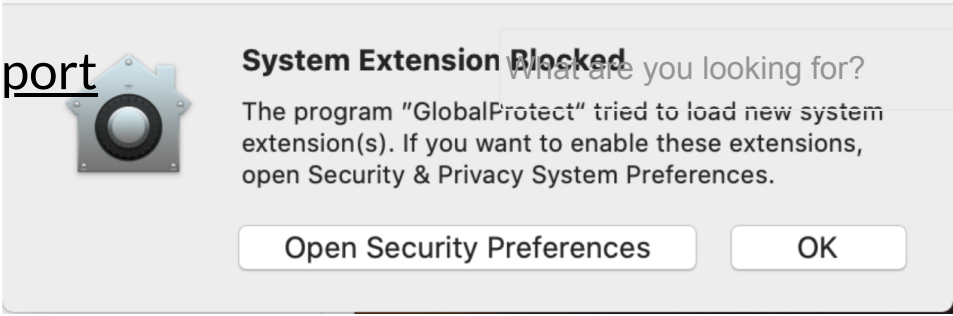
-  [Print](#)
-  [Follow](#)
-  [Copy Link](#)

Attachments

- [GlobalProtectEnforcer.m...](#)
- [GlobalProtectSplitApp.m...](#)
- [GlobalProtectSplitDNS....](#)
- [GlobalProtectSplitDomai...](#)

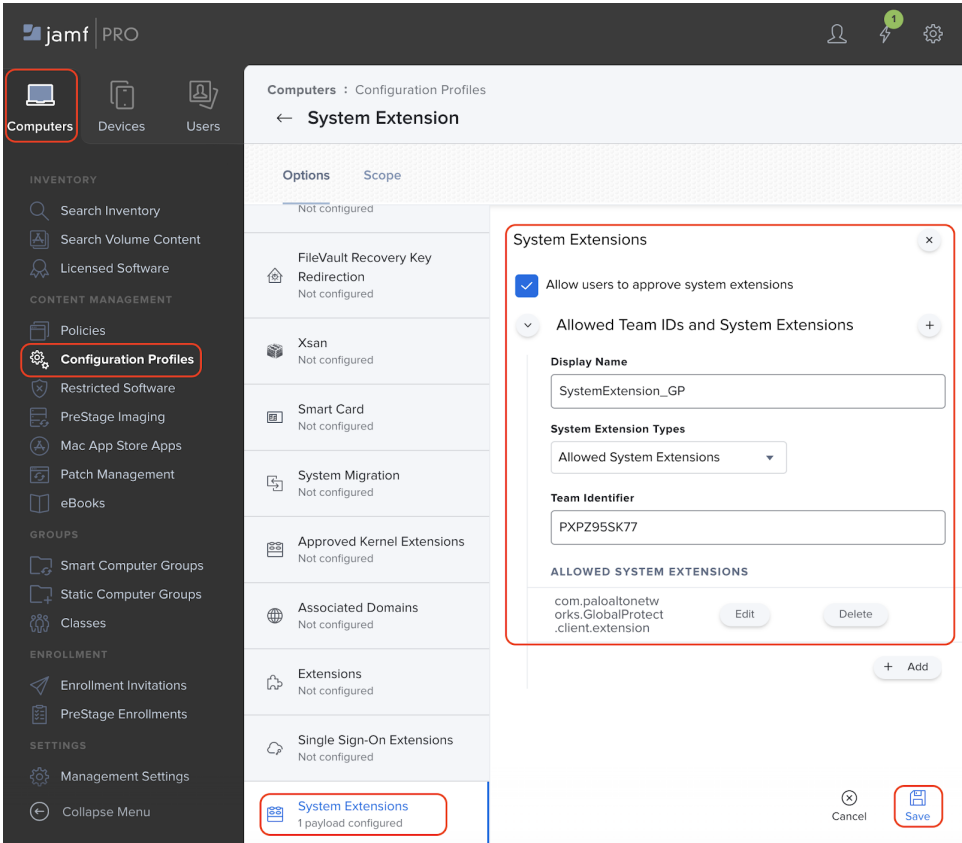
Feedback

Was this information helpful?
 



What are you looking for?

- To enable the System extension, please follow below steps:
 - On jamf PRO, navigate to Computers > Configuration Profiles > New.
 - Here, create a configuration profile as shown below with following information:
 - Select System Extensions.
 - Enter the Team Identifier used by the GlobalProtect app (PXPZ95SK77).
 - Enter the Bundle Identifier (com.paloaltonetworks.GlobalProtect.client.extension).



Note: To enable System Extensions immediately after installation of the GlobalProtect App, use the following command:

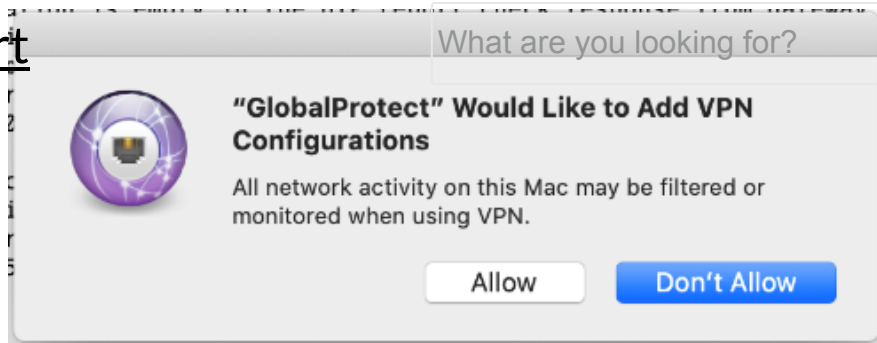
```
sudo installer -pkg GlobalProtect.pkg -applyChoiceChangesXML install_system_extensions.xml -target /
```

The content of install_system_extensions.xml is

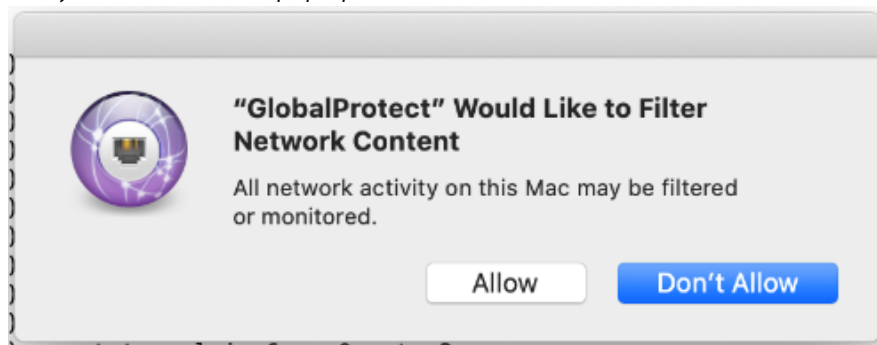
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
  <dict>
    <key>attributeSetting</key>
    <integer>1</integer>
    <key>choiceAttribute</key>
    <string>selected</string>
    <key>choiceIdentifier</key>
    <string>third</string>
  </dict>
  <dict>
    <key>attributeSetting</key>
    <integer>1</integer>
    <key>choiceAttribute</key>
    <string>selected</string>
    <key>choiceIdentifier</key>
    <string>com.paloaltonetworks.globalprotect.systemext.pkg</string>
  </dict>
</array>
</plist>
```

Enable GlobalProtect Network Extension on macOS Catalina 10.15.4 and later Endpoints:

- Upon successful installation of GlobalProtect Client, following network extension pop-ups will be seen as explained in [GlobalProtect app user guide](#).
 - Split-Tunnel application, domain & dns pop-up



b. Enforce GlobalProtect pop-up



- There are 4 different network extension configuration profile files attached to this document which has usage as explained below:

1. GlobalProtectSplitApp.mobileconfig (MD5 Hash = d3d9940daadd91cb8b727db28026910c)

- Configuration profile file specific to GlobalProtect split-tunnel based on application
- Suppresses network extension pop-up (a) related to VPN Configurations

2. GlobalProtectSplitDomain.mobileconfig (MD5 Hash = 235bda0a10eed7ca2b1efe7892439389)

- Configuration profile file specific to GlobalProtect split-tunnel based on domain
- Suppresses network extension pop-up (a) related to VPN Configurations

3. GlobalProtectSplitDNS.mobileconfig (MD5 Hash = 020c721f6fed19cac436e0205eb0bedb)

- Configuration profile file specific to GlobalProtect split-dns feature
- Suppresses network extension pop-up (a) related to Add VPN Configurations

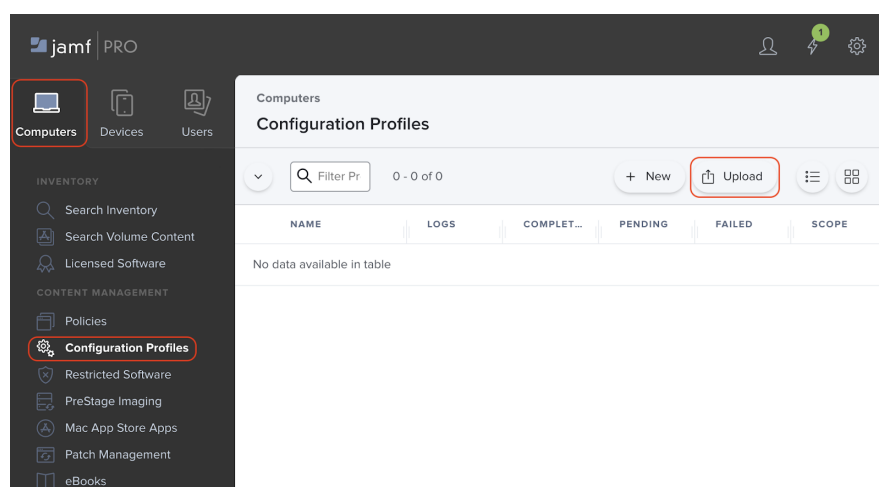
4. GlobalProtectEnforcer.mobileconfig (MD5 Hash = f1e1a501fc70b3a69e29fb5e722983ff)

- Configuration profile file specific to Enforce GlobalProtect feature
- Suppresses network extension pop-up (b) related to Filter Network Content

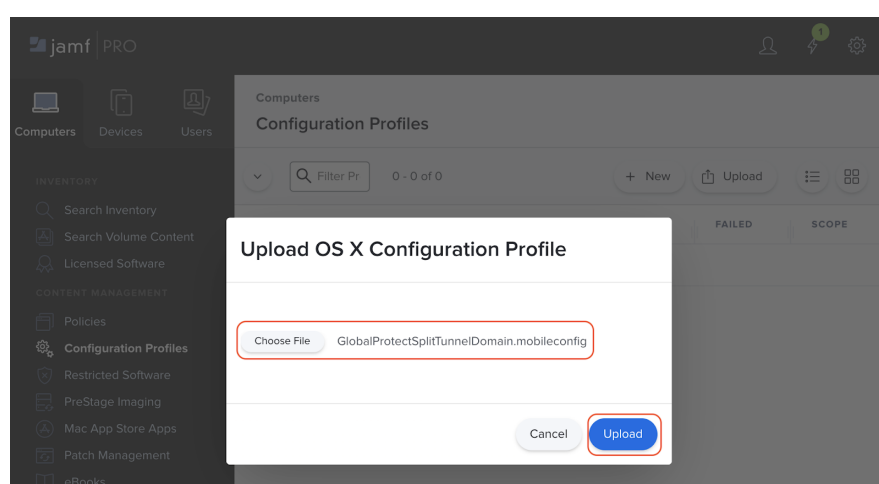
(**Note:** Enforcer mobileconfig provided in this document will not work on jamfPro v10.26.0, but it works on other jamfPro versions. Click [here](#) for steps on how to add Enforcer mobileconfig on jamfPro v10.26.0)

- Following are the step by step instructions on how you can upload and deploy configuration profiles to jamf PRO and deploy them to macOS Catalina endpoints.

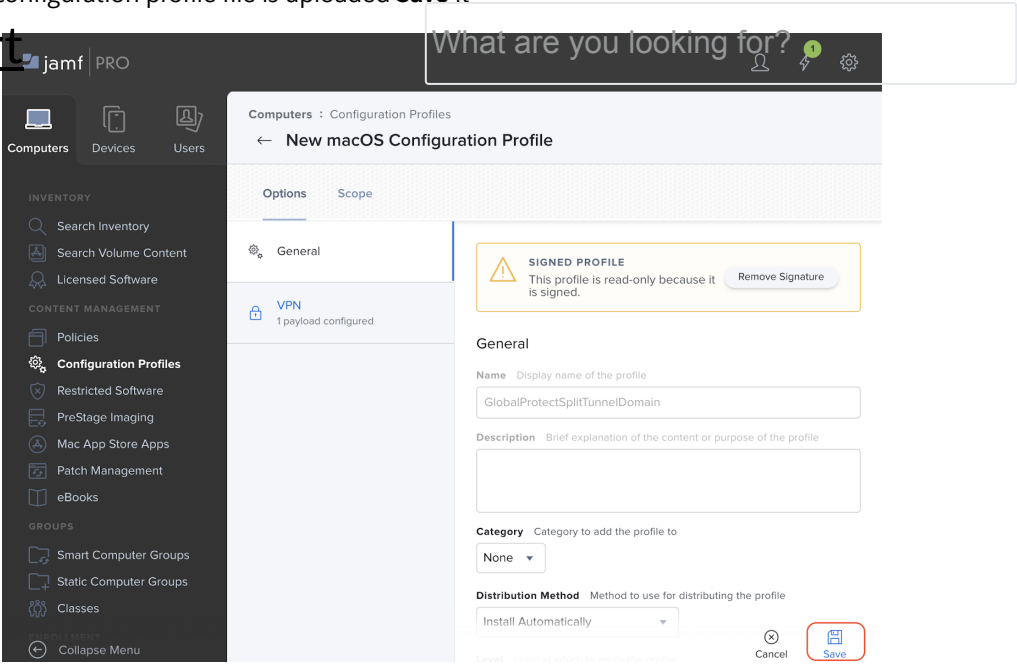
- Once logged in to jamf PRO, navigate to Computers > Configuration Profiles. Here select Upload to choose your mobile configuration file to be uploaded.



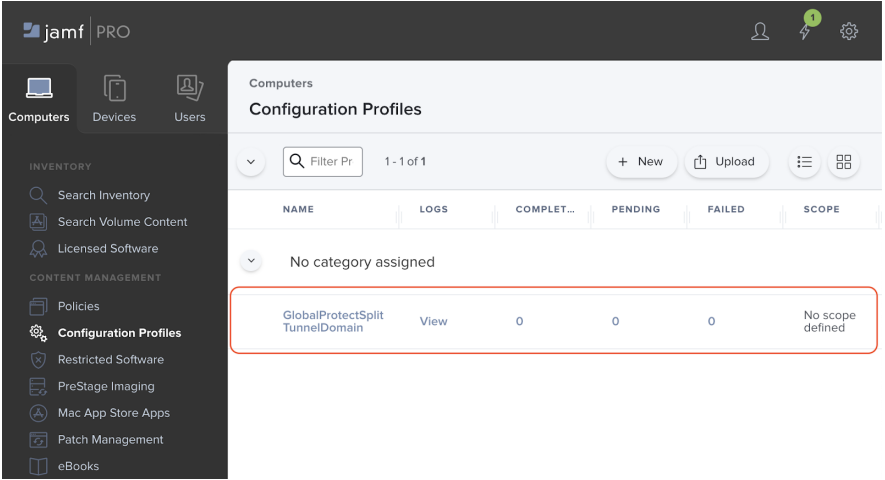
- Select the configuration profile file to be uploaded.



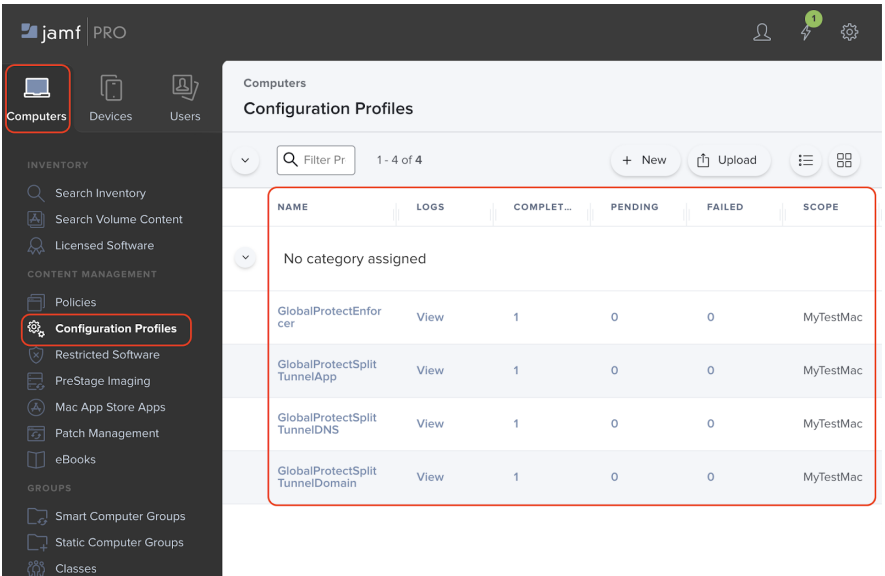
3. Once the configuration profile file is uploaded **Save** it



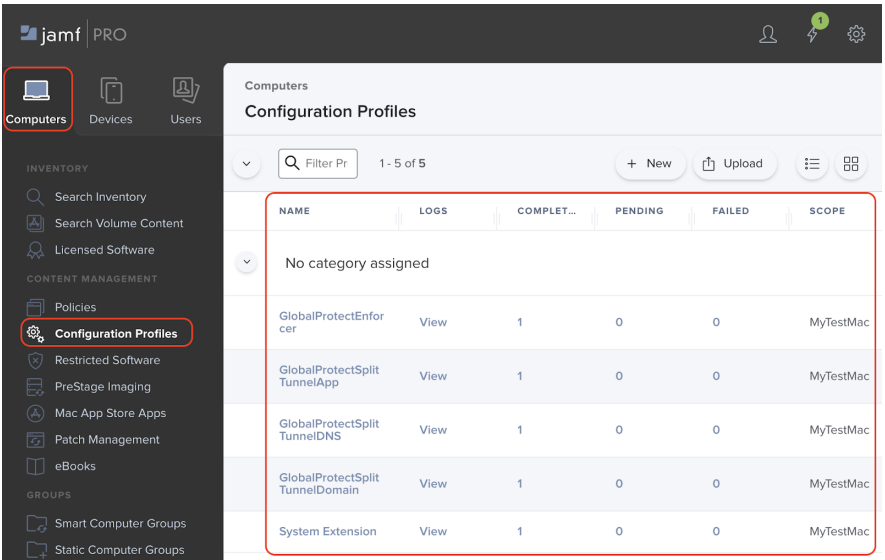
4. Review and verify the configuration profile file is uploaded successfully



5. Repeat steps 1 to 4 to upload any additional configuration profiles required



6. Deploy one or more configuration profiles to your macOS endpoints



Enable GlobalProtect Network Extension on macOS BigSur 11 Endpoints:

- On macOS Big Sur Endpoints, upon successful installation of GlobalProtect Client, following network extension pop-up will be seen as explained in [GlobalProtect app user guide](#).

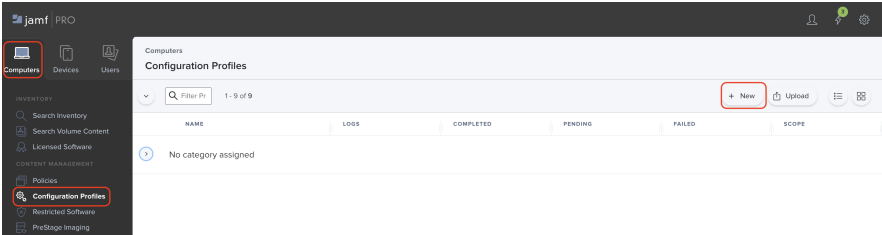


- On macOS BigSur endpoints, a single configuration profile is enough to suppress network extension pop-up unlike macOS Catalina. The steps to add a configuration profile for macOS Big Sur endpoints is the same as the [Steps for adding a configuration profile for Enforcer on jamfPro v10.26.0](#).

Steps for Adding a Configuration Profile for Enforcer on jamfPro v10.26.0.

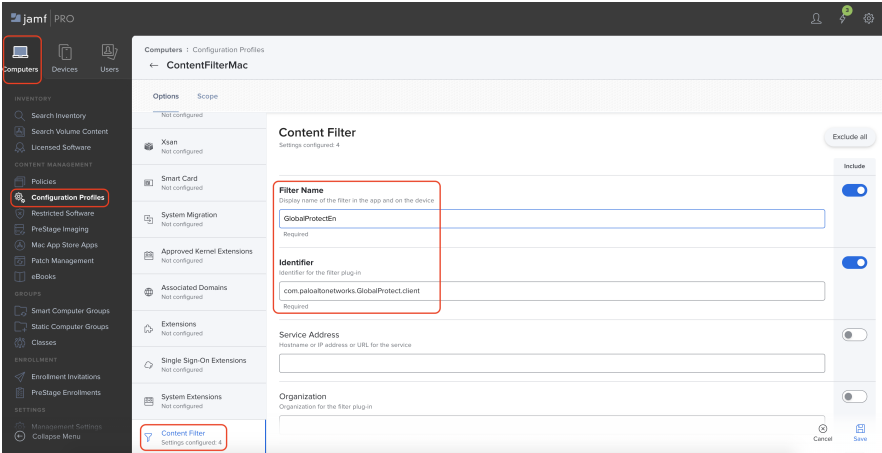
Jamf Pro v10.26.0 introduced the Content Filtering payload for macOS devices. It appears that this work also introduced an issue (JAMF Bug# PI-009162) which prevents the ability to upload profiles that include this payload (for example, GlobalProtect Enforcer mobileconfig), both via the GUI and the API. At this time, the only workaround available is to construct the profile using the GUI that's now available in Jamf Pro v10.26 and later. Following are the steps to configure GlobalProtect Enforcer mobileconfig using the GUI.

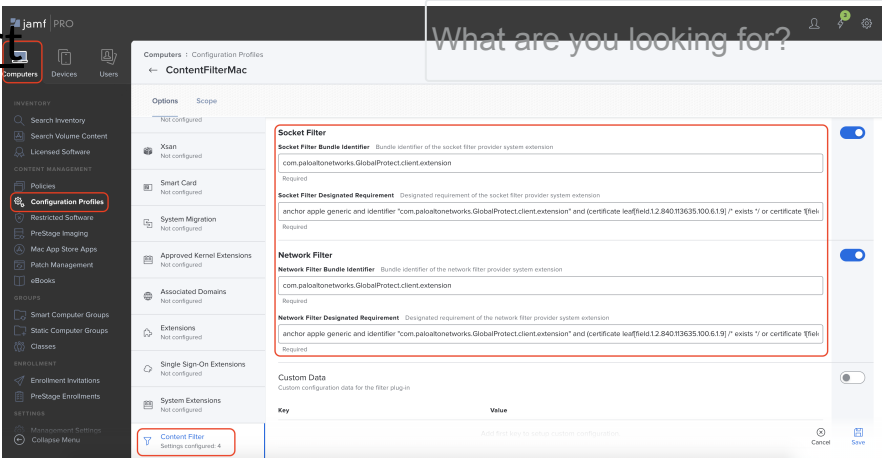
- Once logged in to jamf PRO, navigate to Computers > Configuration Profiles. Select "New" to add configuration profile for GlobalProtect Enforcer.



- Select Content Filter from the options and configure the following values and save the configuration profile.

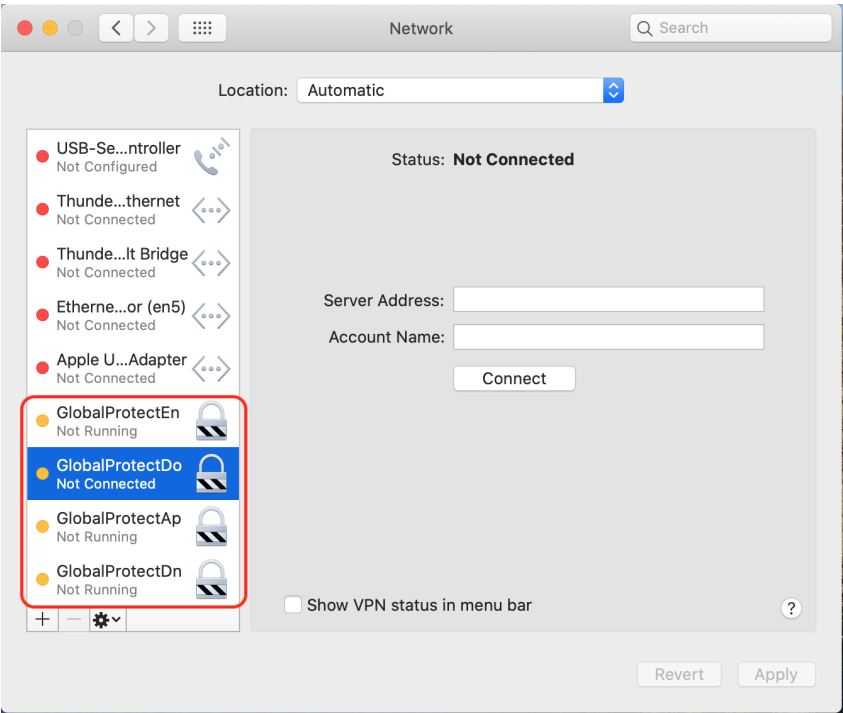
- FilterName** = GlobalProtectEn
- Identifier** = com.paloaltonetworks.GlobalProtect.client
- Socket Filter Bundle Identifier** = com.paloaltonetworks.GlobalProtect.client.extension
- Socket Filter Designated Requirement** = anchor apple generic and identifier "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = PXPZ95SK77)
- Network Filter Bundle Identifier** = com.paloaltonetworks.GlobalProtect.client.extension
- Network Filter Designated Requirement** = anchor apple generic and identifier "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = PXPZ95SK77)



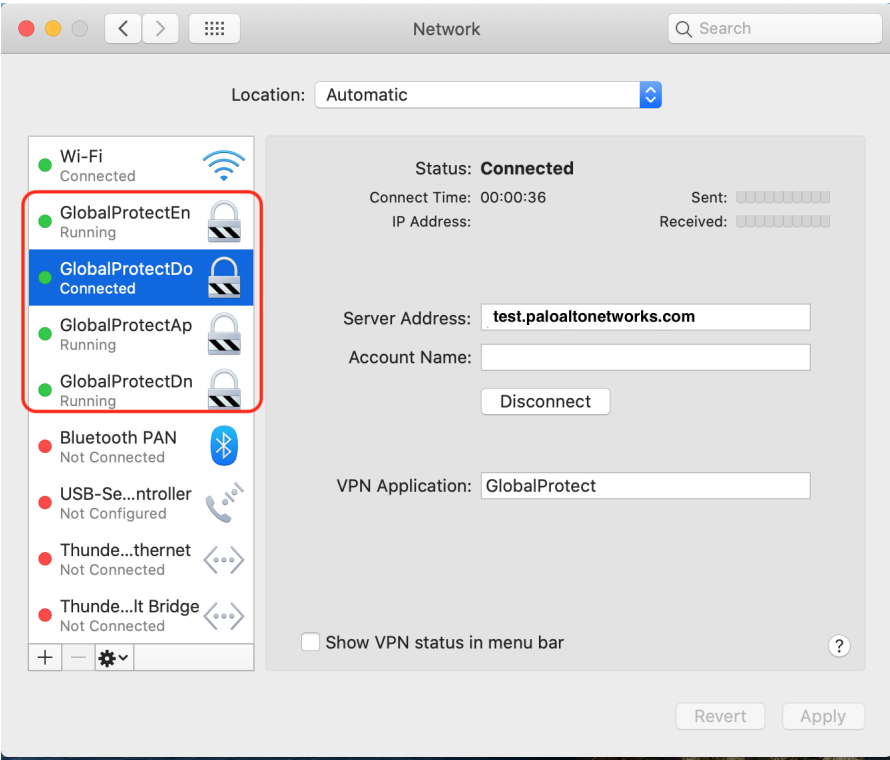


Verify Configuration Profiles:

1. Successfully deployed GlobalProtect configuration profiles on macOS will create one or more of following network interfaces under System Preferences >> Network as shown below:
 - GloblaProtectDo: Network interface for GlobalProtect Domain
 - GloblaProtectAp: Network interface for GlobalProtect Application
 - GloblaProtectEn: Network interface for GlobalProtect Enforcer
 - GloblaProtectDn: Network interface for GlobalProtect DNS



2. Once GlobalProtect VPN tunnel is established network interfaces become active, connected or running, as shown below:



Note: Even though profiles are used to enable System and Network Extensions, the system will still pop up dialog box asking Admin password for removing system extensions during GP uninstallation.

Attachments

- [GlobalProtectEnforcer.mobileconfig](#)
- [GlobalProtectSplitApp.mobileconfig](#)
- [GlobalProtectSplitDNS.mobileconfig](#)
- [GlobalProtectSplitDomain.mobileconfig](#)



Company

Legal Notices

Resources

Customer Support

Careers

Privacy

Terms of Use

What are you looking for?



89+



David Higgs ▾

Live Community

Email Subscription

Beacon